Time Sensitive Information!

These Configuration Changes Must Be Applied
Ten Days Prior to Absolute VOICE Cut-Over

Cisco ASA and Cisco ISR Router Configuration For Absolute VOICE Cloud Telephony Deployment

Document Version 1.1

March 17th, 2017

Table of Contents

Read Me!

1. These changes must be applied before client implements their Absolute VOICE hosted telephony solution.
2. If you are experienced with business class firewalls and routers, please have your IT staff/contractor perform these changes for you.
3. Please read this entire document before attempting to make any changes.
4. If you have questions about this document, you can call 800-955-6703 to schedule an appointment with one of our firewall support specialists. We will attempt schedule your appointment within 24- 48 hours of your call to us so please allow adequate time.
5. After changes are completed please let your client or Absolute VOICE Customer Support specialist know.
6. Once completed, an Absolute VOICE technician will be requesting access or a collaborative web session to verify settings prior to customer cut over.

Introduction

This document is for IT administrators and illustrates configuration changes required on Cisco ASA and ISR firewall & router appliances to support Absolute VOICE's cloud communications telecommunications platform. This document assumes a basic network deployment consisting of one internal LAN network containing the IP phones and one WAN network connected to the Internet. While we strongly recommend a dedicated network for VoIP traffic, the instructions below can be used for a "converged" network whereby both VoIP and non-VoIP traffic share one physical WAN network. With basic modifications (such as adding access rules for additional interfaces); this configuration can be extrapolated for other network layouts. The syntax and configurations below may vary slightly from what is displayed while configuring the device depending on model and IOS software version. Setting values not mentioned may be left at default or changed as required for specific purposes.

Please call Absolute VOICE Customer Support at 800-955-6703 if you need any further information. Firewall changes can be in depth and you will need to schedule time with one of our specialists if you need assistance.

Firewall Checklist

After applying the configurations commands in this document please use one of the following methods to provide router "verification" to Absolute.

Item #:	Configuration:	Completed:
1	Copy configuration into a text file using the following command in the CLI: *Show running-config* (show run)	
Or		
2	Provide a text file with the commands applied to Cisco ASA/ISR	

Cisco ASA

Console or Telnet into the Cisco ASA

ASA - Absolute VOICE recommended settings:

- Note:
  - Set sip inspect to ON for versions above 8.2, otherwise OFF (no sip-inspect)
  - On newer Cisco ASA IOS 9.4 – Disable SIP Inspect
    - The inspect option is set within the: policy-map global_policy

Change into the configuration mode:

```
enable
configure terminal
```

Timers:

```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 1:10:00 sip_media 0:10:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
```

QoS Example:

```
priority-queue inside
priority-queue outside
class-map VOIP
 match port udp range 16000 16999
class-map VOIPinternal
 match port udp range 11780 11800
class-map VOIPSip
 match port udp range sip 5079
class-map inspection_default
 match default-inspection-traffic
class-map DSCP-EF
 match dscp ef
 !
  policy-map PMVOIP
 class VOIP
  priority
 class VOIPinternal
  priority
 class VOIPSip
  priority
 class DSCP-EF
  priority
```

Apply policy to interfaces:

```
service-policy global_policy global
service-policy PMVOIP interface inside
service-policy PMVOIP interface outside
wr
```

Cisco ISR Model Routers

Console or Telnet into the Cisco router

Change into the configuration mode:
enable
configure terminal

If your Cisco ISR router has Cisco security IOS loaded, please enter the following command to disable SIP ALG:
no ip nat service sip udp port 5060
no ip nat service sip tcp port 5060

Create ACL to include Absolute VOICE ports, Class Maps and Policy Maps:
access-list 110 permit udp any range 16000 16999 any
access-list 110 permit udp any range 11780 11800 any
access-list 110 permit udp any eq 5060 any
access-list 110 permit udp any eq 9000 any
access-list 110 permit tcp any eq 5061 any
!
!
priority-list 1 protocol ip high list 110
!
class-map match-all AbsoluteVOICEVoIP
 match access-group 110
 match dscp ef
!
!
policy-map PMAbsoluteVOICEVoIP
 class AbsoluteVOICEVoIP
  priority percent 30
!

Apply Policy to the WAN/External Interface: (note please confirm external interface, may not be fa0/1)
interface fa0/1
description Firewall Outside Interface
  service-policy output PMAbsoluteVOICEVoIP
!
//if security features are enabled for the IOS please enter the following command to disable SIP Inspect
//no ip nat service sip udp port 5060
!
wr

References:

http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a0080103eae.shtml

http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfpq_ps1835_TSD_Products_Configuration_Guide_Chapter.html

http://www.surevoip.co.uk/support/wiki/troubleshooting:sip_alg:cisco_ios

Document Revision History

Version	Reason for Change	Date
1.0 Draft	Initial Draft Document	September 14, 2016
1.1	Firewall Checklist added	March 17th, 2017